Key Exchange Algorithm by Using Quantum Computation

Dr.Samer Saeed Essa*

ABSTRUCT

Quantum computation is a new field bridging many disciplines, including theoretical physics, functional analysis and group theory, electrical engineering, computer science, and quantum cryptography. The goal of this paper is to explore the base of quantum computation that serves to build up a secure algorithm for keys in the unsecured communication channel between two hosts (computers) by applying quantum key exchange algorithm which has highly guarantee protecting toward the computational complexity because the quantum key exchange algorithm is more complex in computation than the classical key exchange algorithm if it perform in classical computer. Also, this algorithm (key exchange algorithm) provides the ability to perform in quantum computer if will be available in future.

* **Al-Mansour University College**

1. Introduction

In particular, quantum mechanics can be used to help solve the key distribution problem, which is encountered by any two entities that wish to communicate using a cryptographically protected channel. If any one want to use a traditional block cipher and message authentication code to protect their communications, they need to agree upon a shared key to use. This problem is currently solved using public-key cryptography algorithm. Each one generates a public-private key pair and registers their public key with a Certification Authority. The Certification Authority then creates a certificate for each of them and distributes the certificate to the other party. They can now use their private keys and the public key contained in each other's certificate to agree upon a shared symmetric key to be used in the block cipher or message authentication code. A number of specific algorithms and protocols exist for doing this. These include key exchange algorithm agreement, RSA algorithm (key transport), etc.

Public-key cryptography algorithm is currently secure. Using key sizes currently in use, it appears infeasible for any attacker to be able to obtain a user's private key solely from his/her public key, which is what would typically be required to break these schemes. However, in theory, if sufficient computing power existed or if a solution is found to the mathematical problem upon which the algorithm is based, then these schemes could be vulnerable to attack. There is no reason to believe that either of these outcomes is likely. However, since the security provided is computational, rather than absolute.

A quantum computer can be implemented using any small particle that can have two states. Quantum computers might be built from atoms that are both excited and not excited at the same time. They might be built from photons of light that are in two places at the same time. They might be built from protons and neutrons that have a spin of "up" and "down" at the same time.

It is widely suspected that if large-scale quantum computers can be built, they will be able to solve certain problems faster than any classical computer. Quantum computers are different from classical computers, such computers are based on transistors, even though these use quantum mechanical effects other than state superpositions [1,2,3].

2. Short Story of Quantum Computing

The story of a computational device based on quantum mechanics was first explored in the 1970's and early 1980's by physicists and computer scientists. The idea emerged when scientists were pondering the fundamental limits of computation. They understood that if technology continued to abide by Moore's Law, then the continually shrinking size of circuitry packed onto silicon chips would eventually reach a point where individual elements would be no larger than a few atoms. Here a problem arose because at the atomic scale the physical laws that govern the behavior and properties of the circuit are inherently quantum mechanical in nature, not classical. This then raised the question of whether a new kind of computer could be devised based on the principles of quantum physics.

The idea of quantum computation started as early as 1982, when the physicist Richard Feynman considered simulation of quantum-mechanical objects by other quantum systems. However, the unusual power of quantum computation was not really anticipated until the 1985 when David Deutsch published a crucial theoretical in which he described a universal quantum computer. After the Deutsch, the hunt was on for something interesting for quantum computers to do. At the time all that could be found were a few rather contrived mathematical problems and the whole issue of quantum computation seemed little more than an academic curiosity.

It all changed rather suddenly in 1994 when Peter Shor devised the first quantum algorithm that, in principle, can perform efficient factorization.

Quantum algorithms require a quantum computer. The first quantum algorithm that can run faster on a quantum computer than on any classical computer was put forward by Deutsch in 1985 and generalized by Deutsch and Jozsa in 1992. The problem they solved–deciding if all possible results of a function are either identical or equally distributed between two values-had little practical relevance.

A very useful algorithm was developed in 1994 by Coppersmith: he showed how the Fourier transform can be implemented efficiently on a quantum computer. The Fourier transform has a wide range of applications in physics and mathematics. In particular it is also used in number theory for factoring large numbers.[2,4]

3. The Basis of Quantum Computing

In quantum mechanics, the state of a physical system (such as an electron or a photon) is described by an element of a mathematical object called a Hilbert space. The realization of the Hilbert space depends on the particular system. For instance, in the case of a single particle system, the state can be described by a complex-valued function defined on R^3 (three-dimensional space) called a wave function. As described in the article on quantum mechanics, this function has a probabilistic interpretation; of particular significance is that quantum states have a property called superposition. A similar realization of the Hilbert space exists for systems of interacting particles. The time evolution of the system state is given by a family $\{U_t\}$ (with t denoting time) of unitary transformations of H. Thus if φ is the state at time 0, then $U_t \varphi$ is the state at time t.

A classical computer has a memory made up of bits, where each bit holds either a one or a zero. The device computes by manipulating those bits, i.e. by transporting these bits from memory to logic gates and back. A quantum computer maintains a set of qubits. A qubit can hold a one, or a zero, or a superposition of these. A quantum computer operates by manipulating those qubits, i.e. by transporting these bits from memory to quantum logic gates and back. Qubits for a quantum computer can be implemented using particles with two spin states: "up" and "down"; in fact any system, possessing an observable quantity *A* which is *conserved* under time evolution and such that *A* has at least two discrete and sufficiently spaced consecutive eigenvalues, is a suitable candidate for implementing a qubit.

A quantum bit, or qubit, is a unit vector in a two dimensional complex vector space for which a particular basis, denoted by {|0>, |1>}, has been fixed. The orthonormal basis |0> and |1> may correspond to the |↑> and |→> polarizations of a photon respectively, or to the polarizations |↗> and |↖>. Or |0> and |1> could correspond to the spin-up and spin-down states of an electron.

For the purposes of quantum computing, the basis states |0> and |1> are taken to encode the classical bit values 0 and 1 respectively. Unlike classical bits however, qubits can be in a superposition of |0>and |1> such as a|0>+ *b* |1> where a and *b* are complex numbers such that $|a|^2 + |b|^2 = 1$. Just as in the photon polarization case, if such a superposition is measured with respect to the basis {|0>, |1>}, the probability that the measured value is |0> is $|a|^2$ and the probability that the measured value is |0> is $|b|^2$. When talking about qubits, and quantum computations in general, a fixed basis with respect to which all statements are made has been chosen in advance. In particular, unless otherwise specified, all measurements are made with respect to the standard basis for quantum computation {|0>, |1>}.[4,5]

4. Quantum bits (qubits)

Consider first a classical computer that operates on a 3 bit register. At a given time, the state of the register is determined by a single string of 3 bits, such as "101". This is usually expressed by saying that the register contains a single string of 3 bits. A quantum computer, on the other hand, can be in a state which is a mixture of all the classically allowed states. The particular state is determined by 8 complex numbers. In quantum mechanics notation we would write:

$$|\psi\rangle = a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle$$

where *a*, *b*, *c*, *d*, *e*, *f*, *g*, and *h* are complex. Let us consider a particular example:

State	Amplitude	Probability
*	(α+i β)	($\|\alpha\|^2+\|\beta\|^2$)
000	*a* = 0.37 + i 0.04	0.14
001	*b* = 0.35 + i 0.43	0.31
010	*c* = 0.09 + i 0.31	0.10
011	*d* = 0.30 + i 0.30	0.18
100	*e* = 0.11 + i 0.18	0.04
101	*f* = 0.40 + i 0.01	0.16
110	*g* = 0.09 + i 0.12	0.02
111	*h* = 0.15 + i 0.16	0.05

For an *n* qubit quantum register, this table would have had 2^n rows; for n=300, this is roughly 10^{90}, more rows than there are atoms in the known universe. Note that these values are not all independent, since the probability constraint must be met. The representation is also non-unique, since there is no way to physically distinguish between this quantum register and a similar one where all of the amplitudes have been multiplied by the same phase such as 1, i, or in general any number on the complex unit circle. One can show the dimension of the set of states of an *n* qubit register is $2^{n+1} - 2$.

The first column shows all classically allowed states for three bits. Whereas a classical computer can hold only one such pattern at a time, a quantum computer can be in a superposition state of all 8 patterns. The second column shows the "amplitude" for each of the 8 states. These 8 complex numbers are a snapshot of the register at a given time. In this sense, a 3-qubit quantum computer has far more memory than a 3-bit classical computer because it can simultaneously represent all possible states of the classical computer.

When the qubit is measured, it is projected onto one of the classically allowed states. The absolute value squared of the amplitude of each classical state gives the probability that the qubit will be measured in that state. Looking at the table, the third column gives the probability for measuring each possible register configuration. In this example, there is a 14% chance that the returned string will be "000", a 31% chance it will be "001", and so on. Each complex number ($\alpha+\beta i$) is called an (complex valued) *amplitude*, and each probability ($|\alpha|^2+|\beta|^2$) is the absolute square of the amplitude, because it equals $|\alpha+ \beta i|^2$. The probabilities must sum to 1.[3,4]

5. Quantum Key Polarization

A photon's polarization state can be modeled by a unit vector pointing in the appropriate direction. Any arbitrary polarization can be expressed as a linear combination a|↑> + b|→> of the two basis vectors |→> (horizontal polarization) and |↑> (vertical polarization).

Since, there are only interested in the direction of the polarization (the notion of "magnitude" is not meaningful), the state vector will be a unit vector, i.e., $|a|^2 + |b|^2 = 1$. In general, the polarization of a photon can be expressed as a|↑> + b|→> where a and b are complex numbers such that $|a|^2 + |b|^2 = 1$. Note, the choice of orthonormal basis is completely arbitrary: any two orthogonal unit vectors will do (e.g. {|↖>|↗>}).

The measurement postulate of quantum mechanics states that each measurement has an associated orthonormal basis with respect to which the measurement projects the quantum state. For example, the probability that $\psi = a|↑> + b|→>$ is measured as |↑> is $|a|^2$ and the probability that ψ is measured as |→> is $|b|^2$. As measurements are always made with respect to an orthonormal basis, all bases will be assumed to be orthonormal. Note that different measuring devices have different associated bases.

Furthermore, measurement of the quantum state will change the state to the result of the measurement. That is, if measurement of ψ = a|↑>+b|→> results in |↑>, then the state ψ changes to |↑> and if the state is measured again with respect to the same basis will return |↑> with probability 1. Thus, unless the original state happened to be one of the basis vectors, measurement will change that state, and it is not possible to know what the original state [6, 7].

6. Quantum Complexity Measurement

Measurement of one or more particles in a quantum system results in a projection of the state of the system prior to measurement onto the subspace of the state space compatible with the measured values. The amplitude of the projection is then rescaled so that the resulting state vector has length one. The probability that the result of the measurement is a given value is the sum of the squares of the absolute values of the amplitudes of all components compatible with that value of the measurement.

Let us look at an example of measurement in a two qubit system. From now on, unless otherwise specified all measurements will be assumed to be measurements of individual qubits with respect to the basis {|0>, *ket* 1}. Any state of a two qubit system can be expressed as a|00>+ b|01>+ C|10>+ d|11>. where a, b, C, and d, are complex numbers such that $|a|^2 + |b|^2 + |C|^2 + |d|^2 = 1$. When the first qubit is measured with respect to the basis {|0>, *ket* 1}, the probability that the result is |0> is $|a|^2 + |b|^2$. Furthermore, if the measurement gives the first qubit as |0>, the state is projected onto the subspace compatible with the measurement, the subspace spanned by |00> and |01>.

The result of this projection is a|00> + b|01>. To get the state of the system after the measurement, renormalize so that the total probability is 1:

$$\frac{1}{\sqrt{|\alpha|^2 + |b|^2}}\left(\alpha|00\rangle + b|01\rangle\right).$$

Measurement gives another way of thinking about entangled particles. Particles are not entangled if the measurement of one has no effect on the other. For instance, the state is:

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Entangled since the probability that the first bit is measured to be |0> is ½ if the second bit has not been measured. However, if the second bit had previously been measured, the probability that the first bit is measured as |0> is either 1or 0, depending on whether the second bit was measured as |0> or |1> respectively. Thus the probable results of measuring the first bit is changed by a measurement of the second bit. On the other hand, the state is not entangled:

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |01\rangle\right)$$

Since $\frac{1}{\sqrt{2}}\left(|00\rangle + |01\rangle\right) = |0\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$

Any measurement of the first bit will yield |0> regardless of whether the second bit was measured. Similarly, the second bit has a fifty-fifty chance of being measured as |0> regardless of whether the first bit was measured or not. Note that entanglement, in the sense that measurement of one particle has an effect on measurements of another particle, is equivalent to our previous definition of entangled states [6, 4, 9].

7. Classical Key Exchange System

In asymmetric or two-key cryptosystems the enciphering and deciphering keys differ in such a way that at least one key is computationally infeasible to determine from the other. Thus one of the transformations E_k or D_A can be revealed without endangering the other.

Secrecy and authenticity are provided by protecting the separate transformations, D_k for secrecy and E_k for authenticity. Illustrates how this principle can be applied to databases, where some users have read-writer authority to the database, while other users have read authority only. Users with read-write authority are given both D_k and E_k, so they can decipher data stored in the data base or encipher new data to update the database.

If E_k cannot be determined from D_k users with read-only authority can be given D_k so they can decipher the data but cannot update it. Thus D_k is like a read-key, while E_k is like a write-key (more precisely the deciphering key describing D_k is the read-key and the enciphering key describing E_k the write-key).

The concept of two-key cryptosystem was introduced by Differ and Hellman in 1976. They proposed a new method of encryption called public-key encryption where in each user has both a public and private key, and two users can communicate knowing only each other's public keys.

In a public-key system each user A has a public enciphering transformation E_A which may be registered with a public directory, and a private deciphering transformation D_A, which is known only to that user. The private transformation D_A is described by a private key, and the public transformation D_A is described by a private key, and the public transformation E_A by a public key derived from the private key by a one-way transformation. It must be computationally infeasible to determine D_A from E_A (or even to find a transformation equivalent to D_A).

In a public-key system secrecy and authenticity are provided by the separate transformations. Suppose user A wishes to send a message M to another user B. If A knows B's public transformation E_B, A can to B in secrecy by sending the ciphertext $C = E_B (M)$. On receipt B deciphers C using B's private transformation D_B, getting.

For authenticity M must be transformed by A's own private transformation D_A. Ignoring secrecy for the moment, A sends $C = D_A (M)$ to B. On receipt, B uses A's public transformation E_A to compute $E_A(C) = E_A (D_A (M)) = M$.[8]

8. Quantum Key Exchange System

In such systems, public key cryptographic mechanisms are used to provide the authentic channel needed for quantum key exchange. The key exchange sub-system, and hence the overall communications system, will be no more secure than the public key authentication mechanism on which it is based. Moreover, any system using quantum key exchange requires a quantum channel (e.g., an optical fiber) between the communicating parties.

Naturally, such a system would not resist active attacks subsequent to private key compromise. It should be mentioned that there exist proposals for quantum public key protocols, where the quantum state of a string of qubits (quantum bits) is used as a key. Storage, distribution and manipulation of these quantum keys, however, require quantum information processing capabilities beyond the reach of current technology.

This system is merely a method for exchanging keys; no messages are involved. The both side in the first publicly choose a finite field $|F_q>$. Then they publicly choose an element $|g> \in |F_q>$ to serve as their "base element" ($|g>$ is preferably, but not necessarily the generator of the group of elements on $|F_q>$). It is a generator of the key. To generate a key, one side chooses a random integer $|a>$ of order of magnitude $|q>$ and keeps it secret, then computes $|g^{a}> \ mod \ |q> \in |F_q>$, and makes that public. Another side chooses his own secret random integer b and makes public $|g^{b}> mod \ |q> \in |F_q>$. The secret key is then $g^{ab} \ mod \ q \in F_q>$. Both them can compute this key. For example, one knows $|g^{b}>$, (public knowledge) and another own secret $|a>$. and use it for further secure communication. On the other hand, only knows $|g>$,, $|g^{a}>$ and $|g^{b}>$, (finding $|a>$ knowing $|g>$ and $|g^{b}>$), there is no way for him to compute $|g^{ab}>$ only knowing $|g^{a}>$ and $|g^{b}>$.

9. Quantum Key Exchange Algorithm

1: Base Element

Step1.1: Sender (A) and Receiver (B) publicly choose a finite field $|F_q>$.

Step1.2: They publicly choose a random element $|g> \in |F_q>$ such that $|g>$ generates a large subgroup of $|F_q>$, preferably of the same order as that of $|F_q>$ itself.

2: Sender Key generation

Step2.1: Sender (A) chooses a secret random integer a **and Convert the** a **chosen number into dirac representation (quantum representation).**

$$a = |a_1, a_2, \ldots\ldots, a_n\rangle$$

Step2.2: Sender computes $|g>^{|a>} \in |F_q>$.

3: Receiver Key generation

Step3.1: Receiver (B) chooses a secret random integer b **and Convert the** b **chosen number into dirac representation (quantum representation).**

$$b = |b_1, b_2, \ldots\ldots, b_n\rangle$$

Step3.2: Receiver computes $|g>^{|b>} \in |F_q>$.

4: Public Key and Secret Key

Step4.1: Make $|g^a>$ and $|g^b>$ public and keep $|a>$ and $|b>$ secret.

Step4.2: Calculation of the secret key $|g^{ab}>$.

5: Secret Key

Step5.1: Receiver computes the secret key $|g^{ba}> = |g^b>^{|a>}$.

Step5.2: Sender computes the secret key $|g^{ab}> = |g^{a}>^{|b}>$.

6: Finally

Step 6.1: Final there are two secret keys in both of sender ($|g^{ab}> = |g^{a}>^{|b}>$) and receiver ($|g^{ba}> = |g^{b}>^{|a>}$).

Conclusions

1. **In this paper introduces the quantum computation principles and quantum key exchange that serve in data security and cryptography.**
2. **Our quantum key algorithm which is more complex in the degree of computational complexity of implementation that serves in security than traditional key exchange algorithm.**
3. **To solve the problems of various implementations in the quantum algorithm methods to be ready in case of building the quantum computer.**
4. **Convert all old, simple and classical algorithms to quantum algorithms and to reuse them as strong algorithms toward high secrecy degree.**
5. **This algorithm is suitable implementation in quantum computer and also is suitable implementation with more complexes in classical or traditional computer.**

Reference

[1]Tim Moses and Robert Zuccherato, "Quantum Computing and Quantum Cryptography"**, 2003.**

[2]Kenneth G. Paterson and Rudiger Schack, "Why Quantum Cryptography"**, University of London, 2004.**

[3]Wikipedia Foundation, **"Quantum Computer"**, Center For Quantum Computation (CQC), 2004.

[4]Jacob West, **"The Quantum Computer"**, 2000.

[5]Graeme Mitchison, **"What is Quantum Computation and What is it Good For"**, University of Cambridge, 2002.

[6]Eleanor Rieffel & Wolfgarg Polak, "An Introduction to Quantum Computer for Non-Physicists**", www.rieffelpal.xerox.com and www.Polak.pal.xerox.com ,1998.**

[7] Andre Berthiaume, "Quantum Computation"**, University of Amsterdam, 1999.**

[8] Dorothy Elizabeth Robling, "**Denning, Cryptography & Data Security"**, CRC Press, 1983

[9]Andrew Steane, "Quantum Computing**", Reports on Department of Physics Vol61. PP117-173, 1998.**

خوارزمية تبادل المفتاح بإستعمال الحسابِ الكمي

د.سامر سعيد عيسى *

المستخلص

الحساب الكمي حقل جديد الذي يجسر العديد مِن المجالاتِ، بضمن ذلك الفيزياءِ النظريةِ، تحليل الوظيفي ونظرية المجموعةِ، الهندسة الكهربائية، عِلْم حاسبات، وعلم التشفيرالكمي. إن هدفَ هذا البحثِ أن تَستكشفَ أساس الحسابِ الكمي التي تَخْدم لتَعزيز وبناء خوارزميةً للمفاتيح في الإتصال الغير آمن بين مضيفين (حاسبات)وذلك من خلال تَطبيق خوارزميةِ تبادل المفتاح الكمي التي لها إلى حدٍ كبير حِماية وضمان بأتجاه التعقيدِ الحسابي لأن خوارزمية تبادل المفتاح الكمي أكثر تعقيداً مِن خوارزميةِ تبادل المفتاح الكلاسيكيةِ إذا تُؤدي (أو تنفذ) في الحاسوبِ الكلاسيكي. أيضاً، هذه الخوارزميةِ (خوارزمية تبادل المفتاح) تُزود القدرةَ للإداء في الحاسوبِ الكمي إذا سيكُون متوفر مستقبلاً.

*قسم هندسة البرمجيات/كلية المنصور الجامعة